WHAT IS CLAIMED IS:

1. An extended key generator comprising:

a plurality of cascade-connected key transform function sections for receiving different keys in units of rounds, and generating extended keys on the basis of the input keys,

each of said key transform function sections comprising:

first key transform means for executing a transform process using a predetermined substitution table on the basis of a first key obtained from the input key; and

extended key computation means for computing the extended key on the basis of a transformed result of said first key transform means, and a second key obtained from the input key.

2. A generator according to claim 1, wherein each of said key transform function sections comprises:

rotate-shift means for rotate-shifting the input key to the left or right, and inputting the rotate-shifted key to the key transform function section of the next round.

3. A generator according to claim 2, wherein a shift amount of said rotate-shift means is relatively prime to the number of output bits of said first key transform means.

4. A generator according to claim 1, wherein each

of said key transform function sections comprises:

input key transform means for transforming the input key using a substitution table, and inputting the transformed key to the key transform function section of the next round.

5. A generator according to claim 1, wherein each of said key transform function sections comprises:

extended transform means for extending and transforming a transformed result of said first key transform means, and inputting the extended transformed result to said extended key computation means.

6. A generator according to claim 5, wherein the extended transformation of said extended transform means is implemented by shifting a predetermined number of bits.

7. A generator according to claim 6, wherein the shift of the predetermined number of bits is implemented by shifting the transformed result to the left by the number of bits half the number of bits of the transformed result of said first key transform means, or the number of bits obtained by adding an integer multiple of the number of bits of the transformed results to the half number of bits.

8. A generator according to claim 1, wherein a computation of said extended key computation means is addition with carry-up.

9. An encryption/decryption unit comprising an

~~extended key generator of claim 1, comprising:~~

~~a data randomization part for encrypting input plaintext on the basis of the extended keys generated by said key transform function sections and outputting ciphertext, and decrypting input ciphertext and outputting plaintext.~~

~~10. A unit according to claim 9, wherein said data randomization part has a plurality of substitution tables for encryption and decryption, and~~

~~some substitution tables of said data randomization part are common to the substitution tables of said first key transform means.~~

~~11. An extended key generation method, comprising the steps of:~~

~~inputting different keys in units of rounds;~~

~~generating a first key from the inputted key;~~

~~transforming the generated first key by using a predetermined substitution table; and~~

~~computing an extended key on the basis of the transformed result and a second key obtained from the inputted key.~~

~~12. A computer readable storage medium which stores a program for making a computer:~~

~~generate a first key from different keys inputted in units of rounds;~~

~~transform the generated first key by using a predetermined substitution table; and~~

compute an extended key on the basis of the transformed result and a second key obtained from the inputted key.

13. A medium according to claim 12, in which stores a program for making the computer rotate-shift the inputted key to the left or right, and input the rotate-shifted key to the next round.

14. A medium according to claim 13, wherein a shift amount of the rotate-shift function is relatively prime to the number of output bits of the first key transform.

15. A medium according to claim 14, in which stores a program for making the computer transform the inputted key using a substitution table, and input the transformed key to the next round.

16. A medium according to claim 12, in which stores a program for making the computer extend and transform the transformed result based on the first key.

17. A medium according to claim 12, wherein the extended transform function is implemented by shifting a predetermined number of bits.

18. A medium according to claim 17, wherein the shift of the predetermined number of bits is implemented by shifting the transformed result to the left by the number of bits half the number of bits of the transformed result of said first key transform

means, or the number of bits obtained by adding an integer multiple of the number of bits of the transformed results to the half number of bits.

19. A medium according to claim 12, wherein the computation of the extended key is addition with carry-up.

20. A computer readable storage medium which stores a program for making a computer:

generate a first key from different keys inputted in units of rounds;

transform the generated first key by using a predetermined substitution table;

compute an extended key on the basis of the transformed result and a second key obtained from the inputted key; and

execute data randomization for encrypting inputted plaintext on the basis of the generated extended keys and outputting ciphertext, and decrypting inputted ciphertext and outputting plaintext.

21. A medium according to claim 20, wherein the data randomization has a plurality of substitution tables for encryption and decryption, and

some substitution tables of the data randomization are common to the substitution tables used in transformation based on the first key.

22. An extended key generator comprising:

a plurality of cascade-connected key transform

~~function sections for receiving different keys in units of rounds, and generating extended keys on the basis of the inputted keys,~~

~~each of said key transform function sections comprising:~~

~~a plurality of extended transform elements that form a parallel circuit, each of said extended transform elements including:~~

~~a constant register for holding a constant,~~

~~XOR computation means for computing an XOR of the constant held in said constant register, and a first key obtained from the inputted key,~~

~~an S box for executing a transform process using a predetermined substitution table on the basis of a value outputted from said XOR computation means, and~~

~~an extended transformer for extending and transforming a transformed result outputted from said S box; and~~

~~extended key computation means for computing extended keys on the basis of the transformed results outputted from said plurality of extended transform elements, and a second key obtained from the inputted key.~~

~~23. A computer readable storage medium which is used in an extended key generator having a plurality of cascade-connected key transform function sections for receiving different keys in units of rounds,~~

and generating extended keys on the basis of the inputted keys,

said medium storing a program for making a computer in said extended key generator implement:

as each of the key transform function sections,

a plurality of extended transform elements which form a parallel circuit, each extended transform elements including:

a constant register for holding a constant,

XOR computation means for computing an XOR of the constant held in said constant register, and a first key obtained from the inputted key,

an S box for executing a transform process using a predetermined substitution table on the basis of a value outputted from said XOR computation means, and

an extended transformer for extending and transforming a transformed result outputted from said S box; and

extended key computation means for computing extended keys on the basis of the transformed results outputted from said plurality of extended transform elements, and a second key obtained from the inputted key.

24. An extended key generator comprising:

a plurality of cascade-connected key transform function sections for receiving different keys in units of rounds, and generating extended keys on the basis of the inputted keys,

each of said key transform function sections comprising:

a substitution part for nonlinearly substituting the inputted key, and outputting the substituted result;

first key transform means for executing a transform process using a predetermined substitution table on the basis of a first key outputted from said substitution part; and

extended key computation means for computing the extended key on the basis of a transformed result of said first key transform means, and a second key outputted from said substitution part.

25. An extended key generation method, comprising the steps of:

inputting different keys in units of rounds;

nonlinearly substituting the inputted key;

transforming a first key obtained from the substitution by using a predetermined substitution table; and

computing an extended key on the basis of a transformed result, and a second key obtained from the substitution.

26. A computer readable storage medium which stores a program for making a computer:

generate a first key from different keys inputted

~~in units of rounds;~~

~~nonlinearly substitute the inputted key;~~

~~transform a second key obtained from the substitution by using a predetermined substitution table; and~~

~~compute an extended key on the basis of a transformed result, and a second key obtained from the substitution.~~

add A1